

Donnelley Financial Solutions

2025 Acceptable and Electronic Use Policy

Internal Use Only

Offices

DONNELLEY FINANCIAL SOLUTIONS

Corporate Headquarters

35 West Wacker Drive

Chicago, Illinois 60601-9703

Copyright

© 2025 DONNELLEY FINANCIAL SOLUTIONS

All rights reserved. Printed in the United States of America.

Information in this document is subject to change without notice.

Trademarks

DONNELLEY FINANCIAL SOLUTIONS, and/or other names/logos referenced herein are either trademarks or registered trademarks of DONNELLEY FINANCIAL SOLUTIONS. Other product and company names mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved

Table of Contents

1 ACCEPTABLE AND ELECTRONIC USE 4

1.1 Expectation of Privacy/Right to Monitor 4

1.2 Electronic Communications Privacy 4

1.3 Remote Access of a Workstation 5

1.3.1 Working from an Alternate Location 5

1.3.2 Remote Access 6

1.3.3 Securing Information on Mobile Devices 7

1.3.4 Mobile Employee Responsibilities 7

1.4 Acceptable Use Policy 7

1.4.1 General Use and Ownership 8

1.4.2 User Password and Account Management..... 8

1.4.3 User Network Access 8

1.4.4 Malicious Code Prevention..... 9

1.4.5 Security of Electronic Email and Communication Services (Webchat)..... 9

1.4.6 Allowed Security Services 10

1.4.7 Laptop / Desktop Security 11

1.5 Clean Desk and Clear Screen 11

1.6 Reporting Suspicious Activities or Security Incidents 12

1.7 Unacceptable Use 12

1.7.1 Unauthorized Activities 12

1.7.2 Unauthorized Usage 13

1.7.3 Unacceptable Network Activities 13

1.7.4 Unacceptable Email Activities (PR.PT-4) 14

Approved by Dannie Combs as part of the Information Security Policy Version 10.0 on 2/28/2025

1 ACCEPTABLE AND ELECTRONIC USE

Objective

This section establishes the rules of conduct for employees and contractors in the use of information systems and the handling of private or confidential data.. Users are expected to comply with applicable Principles of Ethical Business Conduct (PEBC), the Acceptable and Electronic Use governance contained herein, Code of Conduct policies, and the full Information Security Policy (located [here](#)), departmental policies and procedures, and the law. Not knowing or understanding these governing documents does not excuse one's compliance with them.

1.1 Expectation of Privacy/Right to Monitor

While using corporate assets, users should have no expectation of privacy. DFIN may log, review, and otherwise utilize any information stored on or passing through its information systems for the purpose of managing and enforcing the security of our network infrastructure to protect company, employee, and customers' data.

Including, but not limited to examining electronic mail messages, files on company-issued computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through corporate infrastructure or endpoints.

A wide variety of business partners have entrusted their information to DFIN, and all users must safeguard the privacy and security of this information. You may read more about our privacy practices by visiting. <https://www.dfinsolutions.com/privacy-notice/>

1.2 Electronic Communications Privacy

Employees may not use the organization's systems to access, download, or transmit material which is inappropriate, offensive, illegal, or which degrade existing security controls. This includes language that may be disruptive, defamatory, or derogatory, including but not limited to sexual comments or images, racial slurs, or other comments or images that would offend someone based on his or her race, national origin, gender, sexual orientation, religious, or political beliefs or disability.

Users may not transmit any information that is Non-Public (i.e. copyrighted materials, trade secrets, and confidential or proprietary information) without proper authorization. Where possible, the transmission of sensitive and confidential data should be authenticated using digital signatures or encrypted in accordance with encryption policy and standards.

Using Public Generative Artificial Intelligence (AI) programs (i.e. ChatGPT, BARD, OpenAI) for business purposes, using products that incorporate Generative AI technology, using The Onion Router (TOR) or using peer-to-peer browsing technology is strictly

forbidden unless authorize per the AI Responsible Use policy, inclusive of Microsoft CoPilot and other Supply Chain Security approved tools that leverage AI technologies.

Employees shall not download or install any software not listed within the Common [Catalog Software request](#). To obtain new software authorized software that is not on the list, users must go through the procurement process by opening a [Service Now ticket](#)).

Confidential or private information should not be recorded unless authorized. All parties must be notified in advance whenever conversations are being recorded. Users must verify the identity of telephone, conference and chat call participants before communicating confidential or private information.

1.3 Remote Access of a Workstation

Remote control of a DFIN workstation is only permitted by appropriate systems support personnel using methods of remote control approved by GRC and Security.

Users may use sharing/collaboration features of software or other web conferencing tools. Users may not permit others to “take control” of their workstation through such applications, unless it is in the context of receiving support, during a presentation, demo, or training from appropriate systems support personnel. Use of desktop sharing capabilities is not permitted when a workstation is unattended.

Users are not permitted to use software to remotely access or control non-DFIN computers unless it is authorized and for appropriate business purposes

1.3.1 Working from an Alternate Location

Offsite computer usage, whether at home or at other locations require management authorization. Users may only work from geographic locations approved by Management. Usage should be restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures such as listed in section that proscribes Clean Desk and Clear Screen.

Whether employees are in the office or at an alternate work site, all intellectual property developed or conceived of while an employee is attending to Donnelley Financial Solutions business is the exclusive property of Donnelley Financial Solutions. Such intellectual property includes patent, copyright, trademark, as well as all other intellectual property rights as manifested in memos, plans, strategies, products, computer programs, documentation, and other materials and this property must be protected according to this security policy.

Confidential or private information is not to be transmitted to an offsite location, except in a manner consistent with sections covering Removable Media and Securing Information on Mobile Devices. Employees attending to business at alternative work sites should only use Donnelley Financial Solutions provided software and hardware.

When DFIN supplies an employee with software, hardware, information, data, or other materials to perform business remotely, the title to, and all rights and interests to these items, shall remain with DFIN. In such instances, employee possession does not convey ownership or any implication of ownership. Accordingly, all such items must be promptly returned when an employee separates from the organization.

1.3.2 Remote Access

Remote access to the DFIN network is only permitted from DFIN owned or issued equipment (where applicable) unless specifically authorized. Use of VDI (Virtual Desktop Infrastructure) with multifactor authentication (MFA) through normal standard and approval processes is an acceptable alternative that does not require an exception.

Remote access must comply with encryption, authentication and access management standards

Email may be accessed via personal mobile devices (such as smartphones), the personal device must be enrolled in DFINs' Mobile Application Management (MAM) or Mobile Device Management (MDM) system. Administrative or privileged access is not permitted on personal/BYOD equipment that access DFIN systems. Access from personal mobile devices is not allowed to Production, Staging, Testing, Development or other environments that hold or process Client data.

All remote access to information assets will be accomplished utilizing DFIN provided VPN (Virtual Private Network) solution and two factor authentication and/or stronger. All other external facing applications will require appropriate login methods with security appropriate to the content within the application.

1.3.3 Securing Information on Mobile Devices

Confidential or private information must not be stored on mobile computing devices longer than necessary; confidential or private data must be encrypted at rest

Where confidential or private information must be stored on a mobile device, the manner in which it is stored and then destroyed must follow the guidelines established in sections Removable Media and Disposal of Electronic Storage Media on the use of removable media.

1.3.4 Mobile Employee Responsibilities

Users are responsible for the security of their mobile devices. Users must not leave mobile devices unattended and must not allow anyone else (including family) to access DFIN assets or data. Users must not conduct business when connected to a public wireless hotspot or other public network unless they are utilizing DFIN remote access VPN service.

Personnel accessing cardholder data via remote access technology are prohibited from copying, moving, or storing cardholder data to removable media or local hard drives unless required for a specific authorized business need. Users must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or access parameters with any other person without prior approval from Security and GRC

Users must promptly report to their manager and to the Tech Care Center any stolen, “damage to” or “loss of” computer hardware, software, or confidential or private information that has been entrusted to their care.

1.4 Acceptable Use Policy

This section depicts the behaviors that are considered acceptable in the Donnelley Financial Solutions environment.

DFIN assets are intended to facilitate company business. Therefore, primary usage of these assets should be limited to business related purposes. Incidental personal use of DFIN assets is permitted but should be kept to a minimum using language and standards consistent with other forms of business communication.

1.4.1 General Use and Ownership

All employees must be aware that any work product created during their tenure remains the property of DFIN. Users must consider the sensitivity level of the information in which they handle and properly apply the appropriate protection level based on information classification and handling policies.

Employees are responsible for promptly notifying the appropriate manager if they have access to confidential information for which they do not have a business requirement to access.

1.4.2 User Password and Account Management

Users are responsible for all activities performed with their assigned account IDs. Users are responsible for the security of Account IDs and passwords may not be utilized by anyone but the individual to whom they have been issued. (PR.AC-1) (PR.AC-6) (PR.AC-7)

Passwords must be treated as confidential information. Passwords must not be easy to guess and must not be recorded or stored on paper or electronically in clear text. Users must also not divulge their passwords for any reason, including system administrators. If the confidentiality of a password is in doubt, the password must be changed immediately. System administrators must not circumvent the Password Policy for the sake of ease of use. (PR.AC-1) (PR.AC-6) (PR.AC-7)

Users are not permitted to circumvent user interactive password entry with auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Endpoints must be secured with a password protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging off when the computer will be unattended. Users must not disable or alter the screensaver or change the password protection setting. Any changes to policy, require an approved exception. (PR.AC-1) (PR.AC-6) (PR.AC-7) (PR.AC-02)

1.4.3 User Network Access

Connections to the network, either onsite or remotely, are permitted only for DFIN owned assets. Non-DFIN assets are not permitted unless if it is to an isolated

network segment designed for connection by customers of Donnelley Financial Solutions or visitors to Donnelley Financial Solutions facilities.

Masking or “spoofing” of email addresses, IP addresses, or MAC addresses is strictly forbidden unless authorized directly by the CISO.

Users must not establish any communications system that accepts incoming dial-up calls or bridges network connections into the Donnelley Financial Solutions network. Users may not connect wireless access points to the Donnelley Financial Solutions network unless they are approved by Network Engineering and compliant with applicable wireless device security configuration standards.

1.4.4 Malicious Code Prevention

Endpoints connected to the DFIN network must continually run approved anti-virus/anti-malware software with a current database. Frequency of the database updates is determined by standard. Users must not disable the installed security applications or interfere with their scheduled scans or updates. Users must contact the Tech Care Center immediately if their endpoint protection tool reports an alert.

1.4.5 Security of Electronic Email and Communication Services (Webchat)

Email and Webchat should only be used for business purposes, using terms which are consistent with other forms of business communication. Employees must use only approved electronic messaging and webchat applications such as Teams or Zoom. All other communications services are restricted. If there is a valid, documented, approved business justification for usage (e.g. WeChat), the restriction can be allowed if the user opens an “Internet Restriction” Service Now ticket and obtains the necessary attestations and approvals. At which point, the web version should be used for web chat services and accessed only in the course of employee duties. Employees should not install desktop chat clients without authorization. Users must ensure that information forwarded by (especially attachments) is correctly addressed and sent only to appropriate persons.

Customer data may not be transmitted in any manner outside of DFIN, without customer authorization or if it referenced within a contract that has fully executed.

If allowed by contract, data should be sent as proscribed by the contractual provisions or if not proscribed then sent by most secure method available, but never in plain text or over unsecured network.

Private or confidential information should not be transmitted as text in the body of an email. Where it is necessary to transmit private or confidential information by email, the information should be sent as an encrypted attachment and sent to only those who have a business requirement to handle that specific information. Email addresses should be verified before sending attachments with confidential or private information. The attachment of data files to email is only permitted after confirming the classification of the information being sent. Users are responsible for ensuring attachments are free of viruses, malware, or other malicious code.

Users should treat unsolicited emails with caution and should use caution following email best practices and electronic communication. Internal phishing exercises are performed within the DFIN environment regularly to ensure proper security measures are being taken by the end user.

Business confidential email should not be forwarded (including auto-forwarding of email) to personal email addresses (Gmail, Yahoo, Hotmail)

The use of third-party Personal Email addresses (Gmail, Yahoo, Hotmail) for business purposes is restricted and is only permitted by approval from senior management. Also, see section Electronic Communications Privacy, Securing Information on Mobile Devices, and Mobile Employee Responsibilities

1.4.6 Allowed Security Services

Employees may only access websites through standard Donnelley Financial Solutions security services (for example firewalls, approved URL filters). Employees may not bypass Donnelley Financial Solutions security services by any means, including configuring their workstations to use alternative and or proxy servers. Workstations configured to use specific Donnelley Financial Solutions security services may not be reconfigured by employees to use alternative services without prior authorization from Governance Risk and Compliance and Security.

1.4.7 Laptop / Desktop Security

Users should not save or store client confidential data on laptops / desktops. All laptops and desktops with access to private or confidential data must have a standard approved request and configured to allow only services necessary for business functions. The configuration shall be based upon a least privilege access basis, denying all except those services explicitly permitted.

Laptop/desktops and or mobile device reuse must be wiped and reformatted with DFIN image before providing to the next user. New Laptop/desktops and or mobile devices must have a DFIN image. Only authorized users shall have administrative access to Laptops/desktops. There should be no disabling, no reconfiguration, and no uninstallation of DFIN approved software or settings without security approval.

Laptops/desktops in place prior to January 2008 or having operating systems predating Windows 2000 shall be reviewed on a case-by-case basis for upgrade or installation of the personal firewall. Laptops and desktops in place after January 2008 are to have mitigating controls applied on a case-by-case basis.

1.5 Clean Desk and Clear Screen

This section also applies to individuals who work remotely. Where reasonably possible, extra care should be given to protect screens, work area, and meeting conversations from be inadvertently shared with unauthorized personal. The display screens for all systems used to handle confidential or private information must be positioned so that unauthorized persons cannot readily view them through a window, over the shoulder or by similar means.

Approved login procedures must be strictly observed and users leaving their screen unattended must first lock access to their workstation or log off.

Employees must keep their work area clean and orderly. Confidential and private information must not be left unattended (on desks, screens, printers, or any other media including conference room whiteboards). Employees must organize and file information based on the classification level of the information. (PR.AC-2)

Confidential and private information must only be generated in hard copy to the extent necessary to complete normal business operations. All confidential or private information on hard copy (paper) must be destroyed by shredded before disposal. Intermediate work

products related to confidential or private information, such as carbon copies or memo drafts, must also be shredded when final work product is produced. (PR.IP-5) (PR.IP-6)

1.6 Reporting Suspicious Activities or Security Incidents

Users must report any violations of policies, procedures or standards and any activity by staff, consultants, contractors, or guests that may result in the disclosure or destruction of DFIN or customer information assets. Listed below are some common activities that should be reported to IT Help Desk (The Care Center) or Security@Dfinsolutions.com immediately:

1. Recording customer data to removable media when not required by the business process. (PR.PT-2)
2. Using cameras or cell phones equipped with cameras in areas where customer data is being processed.
3. Allowing unauthorized personnel into restricted areas.

In addition to these, any activity that an employee believes could have a negative impact on DFIN assets and/or business activity must be reported.

1.7 Unacceptable Use

This section is representative of behaviors that are considered unacceptable in the Donnelley Financial Solutions environment. It is not intended to be an exhaustive list.

1.7.1 Unauthorized Activities

Under no circumstances is an employee of DFIN authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DFIN resources.

Users must not violate the intellectual or property rights of any person or company such as copyrights, patents, code, or trade secrets.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal and not acceptable behavior. Legal counsel must be consulted prior to export of any material that is in question.

Employees shall not use anonymizer services or peer-to-peer software (e.g., Tor or other tools that bypass security, monitoring or logging controls).

1.7.2 Unauthorized Usage

Users must not attempt to access any data or programs contained on DFIN systems for which they do not have authorization or explicit consent. Users must not leave messages that contain sensitive or confidential information on answering machines or voicemail systems. Users must not disclose sensitive or confidential information in public places.

Users must not intentionally write, compile, copy, propagate, execute, or introduce any malware, viruses or other computer code designed to self-replicate, damage, or otherwise hinder the performance of any DFIN computer system or DFIN's Client system.

Externally supplied removable media must not be used unless authorized and checked for viruses and malware. Attachments to electronic mail must not be executed or opened unless they have been checked for viruses and malware. (PR.PT-2)

1.7.3 Unacceptable Network Activities

Users are prohibited from altering Donnelley Financial Solutions supplied information assets without authorization. This includes the modification of IP or other network configuration settings, installing or removing hardware or software without authorization, or tampering with security tools or endpoint protection. (NIST CSF 1.1) (PR.PT-02) (PR.PT-04)

Users are prohibited from installing network hardware or software that provides network services or that extends or retransmits network services or traffic without approval from the Network Engineering team. Users must not attempt to interrogate or map the internal networks of other companies or organizations. Users must not attach non-DFIN devices to DFIN network without prior authorization.

Users must not modify IP addresses or network configuration settings or add, remove, or modify hardware or software on their DFIN systems without proper authorization and documentation. (PR.AC-5)

1.7.4 Unacceptable Email Activities (PR.PT-4)

Users must not use electronic communication systems for purposes of political lobbying or commercial unless explicitly approved by Donnelley Financial Solutions management. Users should be aware of the inherent risks of all incoming email and should not respond to unsolicited email or open file attachments unless they have been scanned for possible viruses or malicious code.

Users should not attach data files to email without considering the sensitivity of the information being sent and assuring that the file does not contain viruses or other malicious code.

Users may not forge or attempt to forge email messages, or disguise or attempt to disguise their identity when sending email. This is sometimes referred to as “spoofing.” Spoofing is not acceptable unless approved by the CISO.

Users must not participate in the interception, eavesdropping, recording, or altering another person’s email messages or adopt the identity of another person in any message. Users must not send messages that may be construed as a threat or related to acts or instruments of violence. Users must only send Donnelley Financial Solutions data, business partner data to authorized persons who have a need to know. (PR.AC-4) Users must not use “texting” for business purposes, however the use of “Teams Chat” for business purposes is permissible.